(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 817 485 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication
07.01.1998 Bulletin 1998/02

(51) Int Cl.[6]: **H04N 7/16**, H04N 7/167

(21) Application number **97401382.3**

(22) Date of filing: **17.06.1997**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

(30) Priority: **28.06.1996 FR 9608053**

(71) Applicant: **THOMSON Multimedia**
92648 Boulogne Cédex (FR)

(72) Inventors:
- **Campinos, Arnaldo**
  92648 Boulogne Cedex (FR)
- **Fischer, Jean-Bernard**
  92648 Boulogne Cedex (FR)

(74) Representative: **Ruellan-Lemonnier, Brigitte et al**
THOMSON multimedia,
46 quai A. Le Gallo
92648 Boulogne Cédex (FR)

(54) Conditional access system and smartcard allowing such access

(57) The invention relates to a conditional access system allowing a service provider to supply services only to those users who have acquired entitlements to these services.

The services supplied by a service provider consist of an item scrambled by control words. In order to keep the control words secret, they are supplied after having been encrypted with an algorithm with key K.

The entitlements of each user are forwarded in messages commonly denoted EMM (the abbreviation EMM standing for "Entitlement Management Messages").

According to the invention, the key K of the control words encryption algorithm is contained in the EMMs.

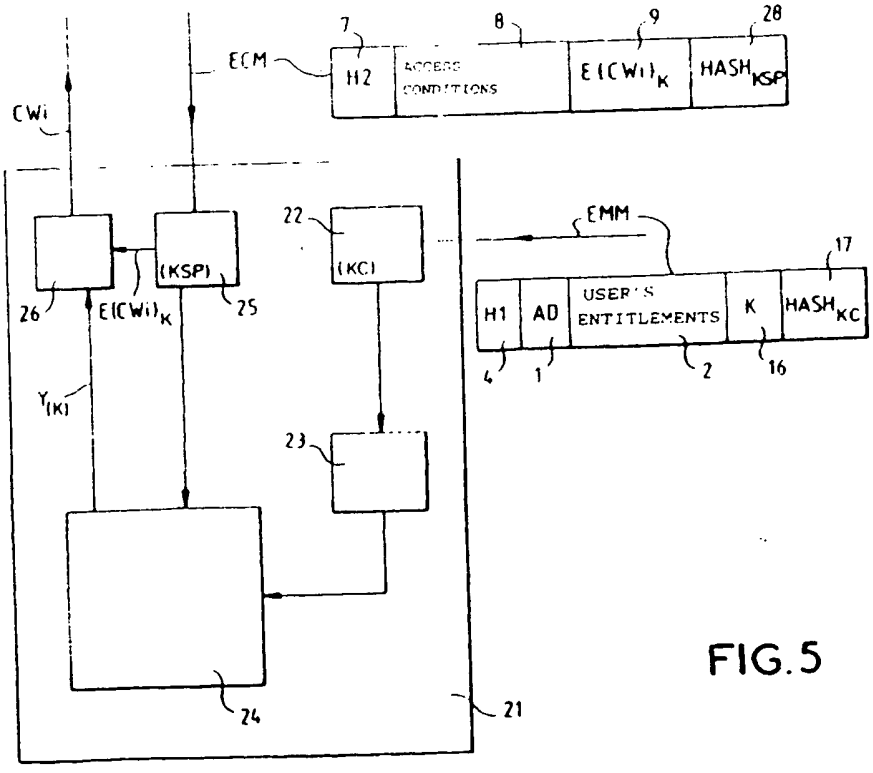

FIG.5

0 817 485 A1

control the validation of the entitlements of the user and a circuit for validating the access conditions associated with the service, the circuit for validating the access conditions containing a second control key. The first control key is different from the key K. According to the preferred embodiment of the invention the first control key is a key individual to the card and hence different from one card to another.

The invention further relates to a conditional access system allowing a service provider to supply services only to the users who have acquired entitlements to these services, the said services consisting of an item scrambled by control words, the said system comprising, for each user, at least one decoder and at least one user card, the said card containing, on the one hand, circuits making it possible to validate and record the entitlements of the user to the service delivered by the provider, the said entitlements being conveyed to the user card by a first message (EMM) and, on the other hand, circuits making it possible to retrieve the control words from the enciphered control words by an algorithm with key K, the said enciphered control words being conveyed to the user card by a second message (ECM). The user card is a card such as that according to the abovementioned invention and the first message (EMM) is a message making it possible to define the entitlements possessed by the user such as that according to the abovementioned invention.

An advantage of the invention is considerably to strengthen the protection of the services supplied by the provider. Piracy in relation to one or more user cards then offers practically no benefit to a would-be pirate any more.

Other characteristics and advantages of the invention will emerge on reading a preferred embodiment given with reference to the appended figures in which:

- Figures 1a and 1b represent respectively a first and a second EMM format according to the prior art;
- Figure 2 represents the format of an ECM according to the prior art;
- Figure 3 represents the schematic of a user card according to the prior art;
- Figures 4a and 4b represent respectively a first EMM format and a second EMM format according to the invention;
- Figure 5 represents the schematic of a user card according to the invention.

In all the figures, the same labels designate the same elements.

Figure 1a represents a first EMM format according to the prior art.

The EMM represented in Figure 1a is composed of a body C1a containing the three main items mentioned earlier, and of a header 4, the content of which (H1) gives, among other things, the type and size of the items contained in the body C1a.

The body C1a consists of a first item 1 containing the address (AD) of the user's card, of a second item 2 containing a description of the user's entitlements, and of a third item 3 containing a cue $HASH_K$. The cue $HASH_K$ depends on the key K and makes it possible to perform the analysis of the EMM mentioned earlier.

Figure 1b represents a second EMM format according to the prior art.

The EMM consists of a header 4 and of a body C1b.

The body C1b consists of the items 5 and 6 containing respectively the address AD of the user card and the description of the user's entitlements enciphered with the algorithm with key K and relating to the address AD ($E(\text{user's entitlements})_{K,AD}$). According to this EMM format, the validation and verification of the entitlements contained in the EMM are performed by the operation of deciphering the enciphered entitlements.

Figure 2 represents the format of an ECM according to the prior art.

The ECM consists of a body C2 and of a header 7 the content (H2) of which gives, among other things, the type and size of the items contained in the body C2.

The body C2 comprises, among other things, a first item 8 containing the set of access conditions associated with the service supplied by the service provider, a second item 9 containing a control word Cwi enciphered with the algorithm with key K ($E(Cwi)_K$) and a third item 10 containing a cue $HASH_K$ depending on the key K and making it possible to validate and verify the content of the access conditions. The control word Cwi represents the current control word, that is to say the control word making it possible to descramble that part of the program which is currently being read.

As is known to those skilled in the art, generally the ECM which contains Cwi also contains a second control word. This second control word is the control word of the next descrambling period, that is to say the current control word of the ECM which has to follow the ECM which contains Cwi as current control word. This second control word has not been represented in Figure 2 so as not to fruitlessly encumber the drawing.

As is known to those skilled in the art, the ECMs are forwarded by the service provider together with the scrambled item IE(ECG).

The ECM format described in Figure 2 is merely one example of an ECM format. In particular, the order of the various blocks (7, 8, 9, 10) making up the ECM described in Figure 2 can be modified.

Figure 3 represents the schematic of a user card according to the prior art.

The user card 11 contains five main circuits:

- a circuit 12 for validating the user's entitlements;
- a circuit 13 for storing the user's validated entitlements;
- a circuit 14 for controlling the access;
- a circuit 15 for validating the ECMs;
- a circuit 27 for deciphering the enciphered control

the user.

If the validated access conditions correspond to the validated entitlements of the user, a signal Y(K) emanating from the access control circuit 24 and applied to the deciphering circuit 26 authorizes the deciphering of the control words. The signal Y(K) contains the key K so as to transmit the latter to the deciphering circuit 26. The enciphered control words $E(Cwi)_K$ are forwarded from the validation circuit 25 to the deciphering circuit 26. The deciphering of the control words is then performed. On completion of the various steps of the deciphering procedure, the deciphered control words Cwi are generated by the deciphering circuit 26 so as to allow the descrambling of the scrambled item.

If the validated access conditions do not correspond to the validated entitlements of the user, the deciphering of the control words is not authorized. According to the invention, validation of a user's entitlements is controlled by a key KC individual to the user or to a group of users. It follows that piracy in relation to a user card can lead only to the jeopardizing of the pirated card itself as well as the user cards of the same group of users if the key KC is shared by one and the same group of users.

Advantageously, all the other user cards remain protected.

According to the above-described embodiment of the invention, the key K is the same for all the services supplied by the provider. The invention allows the implementation of embodiments for which the various services supplied by the provider are scrambled with control words enciphered with an algorithm whose enciphering key differs from one service to another or from one group of services to another.

This is particularly advantageous in the case of systems commonly referred to as "off-line" systems for which the scrambled item IE(ECG) and the ECMs are contained on stand-alone data media such as, for example, CDs ("Compact Discs"), DVDs ("Digital Video Discs") or else CD-ROMs ("Compact-Disc Read Only Memories").

Advantageously, piracy in relation to a user card is then even more devoid of benefit than in the case in which all the services of the provider are scrambled with control words enciphered with the same key K. Thus, piracy in relation to a user card then leads to only very partial access in respect of the various services supplied by the provider.

Scrambling various services, such as for example films, with an algorithm whose keys differ from one service to another cannot be envisaged within the framework of prior art conditional access systems for which the key of the algorithm for enciphering the control words of a service and the key associated with the algorithm for validating the user's entitlements are identical.

Thus, the service provider would then have to supply each user with a card individual to each service or group of services. Such a proliferation of cards is unrealistic, both for practical reasons and for cost reasons.

Generally, regardless of the embodiment of the invention that is to say whether the various services supplied by the provider are associated with a single key for enciphering the control words K or with different enciphering keys K_j (j = 1, 2, . . . m), the invention relates equally well to conditional access systems of the "off-line" type as to conditional access systems of the "on-line" type for which the scrambled item IE(ECG) is an item consisting of a signal dispensed simultaneously to the various customers of the service provider from a single source.

Claims

1. Message (EMM) making it possible to define the entitlements (2) which a user possesses to a service consisting of an item (IE (ECG)) scrambled with the aid of control words (Cwi), the said control words being supplied to the user after having been enciphered by an algorithm with key K, the said message (EMM) containing an item making it possible to validate this message and to verify that the entitlements which the latter contains are the entitlements reserved for the user, the said item making it possible to validate the message and to verify the entitlements which the latter contains being controlled by a key (KC), characterized in that the message contains the key K of the algorithm for enciphering the control words.

2. Message (EMM) according to Claim 1, characterized in that the key (KC) controlling the item making it possible to validate this message and to verify the entitlements which the latter contains is different from the key K of the algorithm for enciphering the control words.

3. Message (EMM) according to Claim 1 or 2, characterized in that the key (KC) controlling the item making it possible to validate this message and to verify the entitlements which the latter contains is individual to each user or group of users.

4. Process making it possible to descramble a scrambled service (IE(ECG)) supplied to at least one user, the said service being scrambled with the aid of control words (Cwi), the said process comprising a step making it possible to supply the user with a first message (ECM) containing at least one control word enciphered with an algorithm with key K, a step making it possible to supply a second message (EMM) containing the entitlements of the user and a step making it possible to validate and verify that the entitlements contained in the second message (EMM) are the entitlements reserved for the user, characterized in that the key K is dispensed to the user in the second message (EMM).

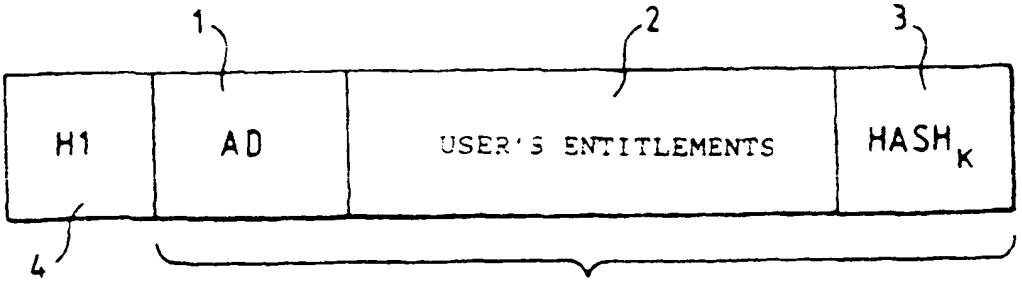

FIG.1a

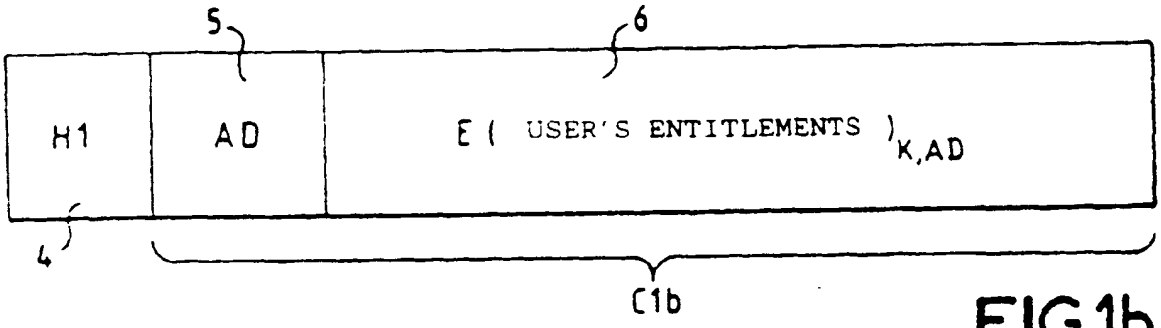

FIG.1b

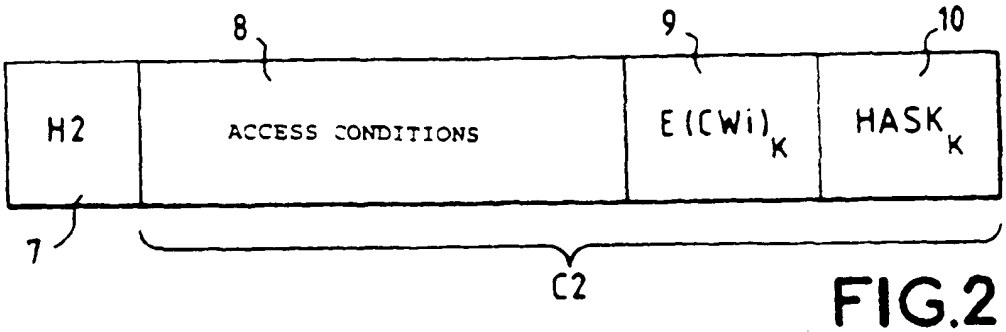

FIG.2

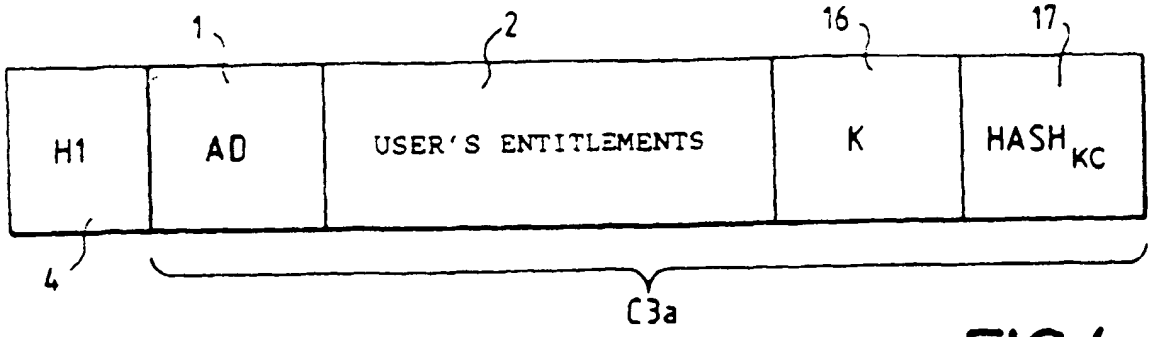
1
2
16
17
H1
AD
USER'S ENTITLEMENTS
K
HASH KC
4
C3a

FIG.4a

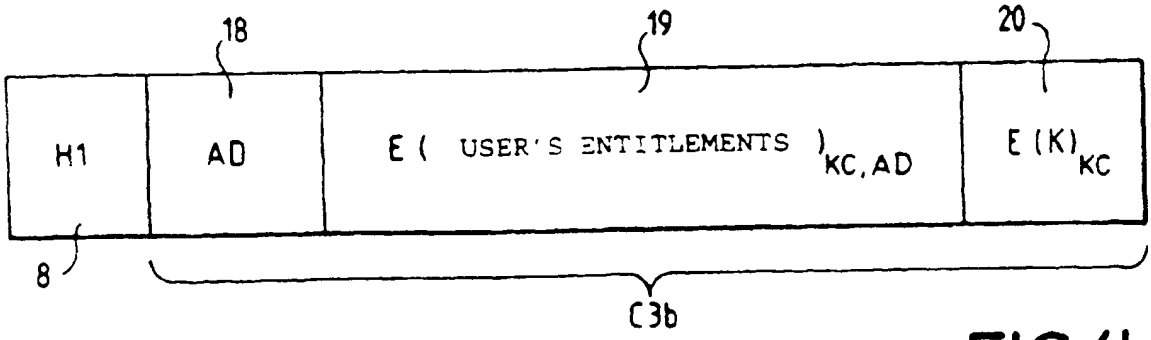
18
19
20
H1
AD
E (USER'S ENTITLEMENTS) KC, AD
E (K) KC
8
C3b

FIG.4b

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 97 40 1382

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	EP 0 506 435 A (SCIENTIFIC ATLANTA) 30 September 1992 * page 8, line 41 - page 13, line 13 * * figures 7-10 *	1-12	H04N7/16 H04N7/167
A	EP 0 461 029 A (MATRA COMMUNICATION ;FRANCE TELECOM (FR); TELEDIFFUSION FSE (FR)) 11 December 1991 * page 4, column 4, line 24 - page 6, column 8, line 4 * * figures 2,3 *	1-5,10	
A	EP 0 375 539 A (EUROP RECH ELECTR LAB) 27 June 1990 * page 3, column 4, line 5 - page 4, column 6, line 38 * * page 5, column 7, line 31 - column 8, line 11 * * figures 1-5 *	7-12	
A	WO 95 28058 A (FRANCE TELECOM ;TELEDIFFUSION FSE (FR)) 19 October 1995 * page 4, line 9 - page 5, line 28 * * page 11, line 4 - page 15, line 34 * * figures 4-9 *	1-6	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04N

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	17 September 1997	Van der Zaal, R

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document